Access to Government Information: An Overview

Updated December 18, 2023

Congressional Research Service
https://crsreports.congress.gov
R47058

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

Access to Government Information: An Overview

Congress has long recognized the people's right to know about the operations and actions of the federal government. A series of modern statutes provides a framework for ways the public may access government information. Built up over the past 60 years, these key statutes allow the public to access information about the federal government's operations, information the government might collect on individuals, and insight into some of the government's decisionmaking processes.

These key statutes include the

- Freedom of Information Act (FOIA; 5 U.S.C. §552),
- Privacy Act of 1974 (Privacy Act; 5 U.S.C. §552a),
- Government in the Sunshine Act (Sunshine Act; 5 U.S.C. §552b), and
- Federal Advisory Committee Act (FACA; 5 U.S.C. Chapter 10).

These statutes generally operate by using one or two access mechanisms: a request-based system for information, and proactive or contemporaneous disclosure of the information in an open forum. Each method has its benefits and drawbacks for individuals seeking to gain information from federal government actors. Implementation and understanding of these statutes and corresponding policies have changed over time.

After enactment of these statutes and subsequent evolution in their implementation, Congress has continued to question whether they provide for sufficient public inspection of government activity and whether federal government actors are complying with or circumventing the intent of these statutes. To help determine whether or not information can be sufficiently accessed, Congress might evaluate multiple questions, including whether the sought-after information is exclusive to certain individuals or software, at what point the information can be retrieved during decisionmaking processes, and if the information provided is sufficient to determine the context in which it was created. This report provides an overview of each of the four statutes and includes a discussion of policy questions and legislative considerations for each one.

SUMMARY

R47058

December 18, 2023

Meghan M. Stuessy
Analyst in Government Organization and Management

Contents

Tables

Contacts

Congress has long recognized the people's right to know about the operations and actions of the federal government. Advocates of open government have often quoted James Madison, considered the Father of the Constitution, who wrote:

> A popular Government without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both. Knowledge will forever govern ignorance; And the people who mean to be their own Governors, must arm themselves with the power, which knowledge gives.[1]

During consideration of amendments to the 1946 Administrative Procedure Act (P.L. 79-404), which laid the groundwork for modern access-to-government-information laws, the Senate highlighted Congress's intent to respond to Madison's writing:

> At no time in our history has this been truer than it is today, when the very vastness of our Government and its myriad of agencies makes it so difficult for the electorate to obtain that "popular information" of which Madison spoke. Only when one further considers that hundreds of departments, branches, and agencies are not directly responsible to the people, does one begin to understand the great importance of having an information policy of full disclosure.[2]

Since the 1960s, Congress has legislated four key statutes which provide access to government information:

1. Freedom of Information Act (FOIA; 5 U.S.C. §552);
2. Privacy Act of 1974 (Privacy Act; 5 U.S.C. §552a);
3. Government in the Sunshine Act (Sunshine Act; 5 U.S.C. §552b); and
4. Federal Advisory Committee Act (FACA; 5 U.S.C. Chapter 10).

Under these statutes, the public may access information through two approaches. The first approach consists of placing a request with the federal government in which an interested party requests information from the government (FOIA; Privacy Act). Members of the public may request documents from agencies or information collected on themselves under these statutes.

The second approach consists of proactive or contemporaneous disclosure by the government in which meetings or information are transparently available for public inspection (Sunshine Act; FACA).[3] FOIA contains elements of both approaches.

[1] Letter from James Madison, former President, to W. T. Barry, August 4, 1822, https://www.loc.gov/resource/mjm.20_0155_0159/?sp=1&st=text.

[2] U.S. Congress, Senate Judiciary, *Clarifying and Protecting the Right of the Public to Information and for Other Purposes*, report to accompany S. 1666, 88th Cong., 2nd sess., July 22, 1964, Report No. 1219, p. 8.

[3] Other statutes provide additional means for public access to federal government information in narrower areas of federal government activity without a need to formally request the information. These include statutes that govern rulemaking and budgeting, among others. For discussion, see CRS In Focus IF10003, *An Overview of Federal Regulations and the Rulemaking Process*, by Maeve P. Carey; and "Congress Evolving in the Face of Complexity: Legislative Efforts to Embed Transparency, Participation, and Representation in Agency Operations," by Clinton T. Brass and Wendy Ginsberg, in CRS Committee Print CP10000, *The Evolving Congress: A Committee Print Prepared for the Senate Committee on Rules and Administration*, coordinated by Walter J. Oleszek, Michael L. Koempel, and Robert Jay Dilger. Other laws govern stewardship of agency information, including but not limited to the Federal Records Act. See CRS In Focus IF11119, *Federal Records: Types and Treatments*, by Meghan M. Stuessy. The topic of congressional access to government information is addressed in CRS Report RL30240, *Congressional Oversight Manual*, coordinated by Christopher M. Davis, Todd Garvey, and Ben Wilhelm.

Key Concepts

The laws discussed in this report represent different approaches to managing and receiving government information. While each statute contemplates access mechanisms in specific contexts, all rely on terms that provide a common understanding to the concept of open government. This section briefly considers the conceptual definition of *government information* compared to other types of information, explores what it means for a user to access information, and concludes with a discussion of the information life cycle as a structure to manage information at different stages.

What Is Government Information?

There is no overarching definition of *government information* in statute. However, the Office of Management and Budget's (OMB's) *Circular No. A-130*, which concerns "Managing Information as a Strategic Resource," defines *information* as "any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms."[4] Agency heads and chief information officers (CIOs) have certain statutory responsibilities to manage information resources, which are also discussed in part within *Circular No. A-130*.[5]

The Federal Records Act (44 U.S.C. Chapters 21, 29, 31, and 33) discusses a particular type of government information, *federal records*, as having value for future preservation. When the information's content is assessed and found to meet certain criteria, it is considered to be a federal record. *Federal record* is defined under the Federal Records Act as

> all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.[6]

Broadly, government agencies and employees have specific legal obligations related to the retention of federal records based on their assessed value.[7]

Government information, thus, may be construed to be recorded information, such as facts, data, or opinions, that were created or received by a component of the federal government when conducting public business.

[4] OMB, *Circular No. A-130: Managing Information as a Strategic Resource*, July 28, 2016, p. 29, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf#page=29. *Circular No. A-130* establishes general policy for information governance, acquisitions, records management, open data, workforce, security, and privacy.

[5] 44 U.S.C. §3506. These responsibilities include, but are not limited to, implementing methods for collecting and analyzing digital information; establishing goals for improving information resources management's contribution to program productivity, efficiency, and effectiveness; and implementing and enforcing requirements for archiving information maintained in electronic format, particularly during the planning, design, and operation of information systems.

[6] 44 U.S.C. §3301.

[7] For more information about federal records and the process to assess federal records for permanent or temporary preservation, see CRS In Focus IF11119, *Federal Records: Types and Treatments*, by Meghan M. Stuessy.

What Is Access?

In practice, the concept of access is multidimensional. Access to information may mean increasing the volume of available information and the variety of formats in which the information is presented. For example, the FOIA Improvement Act of 2016 (P.L. 114-185) amended FOIA to require the proactive disclosure of information in a public and electronically accessible format and mandated the creation of an electronic portal of requested information, among other changes.

Assessing Access

The authors of the major legislation addressing access to government information weighed many factors when considering how the statutes may be applied. Government entities acting under the statutes must also constantly consider these factors:

- Who can access the information, and what tools or software are needed to do so?
- What is the process for requesting or accessing the information? What burden does the process put on requesters and federal agencies? Is the process more burdensome or difficult than it needs to be?
- When can the information be accessed? For what length of time is the information available?
- Are the formats and materials on which the information is recorded and stored being properly preserved? Do they need repair or modernization?
- Is the information provided with sufficient context to understand the full scope of the content? Are only certain people or professionals able to understand the information?

Information Life Cycle

Government information policy has grappled with the concept of access. The term *information life cycle* describes the movement and impact information makes throughout its usable period.

The information life cycle concept, according to the National Archives and Records Administration (NARA), OMB, and others, describes the ways in which information moves and is a method of understanding how laws and policies affect the use of information in the government. Generally, the information life cycle can be thought of as comprising three stages: (1) creation or receipt, (2) maintenance and use, and (3) disposition or destruction of the information.[8] The stage in which the requested information currently resides impacts whether and in what format the requested information may be provided. For example, information being collected by the federal government from individuals under an assurance of confidentiality might have specific limitations on future sharing. Information that is currently in use by a government agency to formulate and debate a policy may be considered pre-decisional and therefore unavailable. Government access laws do not require agencies to respond to requests for information that was never created or already destroyed.

[8] NARA, *Guide to the Inventory, Scheduling, and Disposition of Federal Records: Records Disposition Overview*, https://www.archives.gov/records-mgmt/scheduling/rdo. *OMB Circular A-130* provides additional terminology on the information life cycle. However, this definition is compatible with the simplified NARA definition used in the text of this report. A-130 reads, "'Information life cycle' means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion." OMB, *Circular No. A-130*, p. 29.

Public Access Laws

Congress increasingly considered legislation on the transparency and management of government information in the 1960s and 1970s. Legislators sought to make the executive branch's operations open and available for public inspection, just as Congress's consideration of legislation is available.[9] Members determined that information policies promoting disclosure would enhance government accountability, which was an important goal of the Administrative Procedure Act.[10] Some Members highlighted the changing landscape of government functions and how computers and digital information might change the nature of government services:

> Somehow, the varied and wide-ranging functions which have been thrust very rapidly upon the Federal management machinery of an earlier time have left great loopholes for the gathering, use and disclosure of information about Americans in ways and for reasons that should give us serious pause. The advent of computer technology and new ways of information storage and sharing which have made it possible for government to provide new services and to carry out new programs, have also encouraged the extension of some practices of doubtful wisdom or constitutionality.[11]

Through these debates, as previously noted, Congress enacted statutes that generally operate by using one of two access mechanisms: a request-based system for information from the government and proactive or contemporaneous disclosure of certain information in an open forum.

The results thus far of this legislative debate include four key statutes:

1. the Freedom of Information Act (1966),
2. the Privacy Act (1974),
3. the Government in the Sunshine Act (1976), and
4. the Federal Advisory Committee Act (1972).

The Freedom of Information Act

The Freedom of Information Act establishes a presumption that the public should have access to information in the possession of executive branch agencies and departments of the federal government. Prior to FOIA, a requester had the burden of proof to show a "need to know" to gain access to government information. FOIA assumes a "right to know" and shifts the burden to the federal government to establish a need to keep the information secret.[12]

Government-wide, agencies received 838,164 FOIA requests in FY2021. The top five agencies that received the most FOIA requests were (1) the Department of Homeland Security, (2) the

[9] Rep. Dante Fascell, "Conference Report on S. 5, Government in the Sunshine Act," House debate, *Congressional Record*, vol. 122 (August 31, 1976), p. H28474.

[10] Sen. Edward V. Long, "Amendment of Administrative Procedure Act," Senate debate, *Congressional Record*, vol. 110 (July 28, 1964), p. S17087. The Administrative Procedure Act (APA) of 1946 (5 U.S.C. §551 et seq.) was originally written to bring regularity and predictability to agency decisionmaking, and it provides for, among other things, both formal and informal rulemaking. For more information about the APA and the rulemaking process, see CRS Report RL32240, *The Federal Rulemaking Process: An Overview*, coordinated by Maeve P. Carey.

[11] Sen. Samuel J. Ervin, "Protection of the Right of Privacy," Senate debate, *Congressional Record*, vol. 120 (November 21, 1974), p. S36981.

[12] U.S. Congress, House Committee on Oversight and Government Reform, *A Citizen's Guide to Using the Freedom of Information Act and the Privacy Act to Request Government Records*, committee print, 112th Cong., 2nd sess., September 21, 2012, H.Rept. 112-689, p. 2, https://www.congress.gov/112/crpt/hrpt689/CRPT-112hrpt689.pdf.

Department of Justice (DOJ), (3) the Department of Defense, (4) the Department of Health and Human Services, and (5) the Department of Veterans Affairs.[13]

Any person may make a request for information under FOIA. The statute does not specify that a particular form must be used to make a request. Rather, the request must be in writing and reasonably describe the records sought.[14] Depending on the entity making the request and the scope of the information sought, certain requests may be subject to the assessment of fees to recoup agency staff and information reproduction costs.[15] Many agencies also proactively make information available on their FOIA library pages and may have already published relevant records. DOJ has provided a web portal to allow for the searching of agency resources at https://www.foia.gov/#learn-more.

FOIA establishes a three-part system that requires federal agencies to disclose a large swath of government information to the public.[16] Two of the three parts require a government agency to proactively disclose certain information. First, FOIA directs agencies to publish substantive and procedural rules, along with certain other important government materials, in the *Federal Register*.[17] Second, agencies must electronically disclose a separate set of information that consists of, among other things, final adjudicative opinions and certain "frequently requested" records.[18]

The third part is FOIA's request-based system of disclosure. Any member of the public may request existing government information from covered federal agencies.[19] However, FOIA's presumptive right of access is limited when the requested information falls within the scope of nine statutory exemptions. The nine statutory FOIA exemptions (5 U.S.C. §552(b)) that allow agencies to withhold information are

1. National defense or foreign policy information properly classified pursuant to an executive order;[20]
2. Information related solely to the internal personnel rules and practices of an agency;
3. Data specifically exempted from disclosure by certain statutes;
4. Trade secrets and commercial or financial information obtained from a person that is privileged or confidential;
5. Inter- or intra-agency materials that would not be legally available to a party other than an agency in litigation with the agency;
6. Personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

[13] CRS analysis of FOIA data located at https://www.foia.gov/data.html.

[14] DOJ, FOIA.gov, http://www.foia.gov/faq.html.

[15] For more information about FOIA fees, see CRS In Focus IF11272, *Freedom of Information Act Fees for Government Information*, by Meghan M. Stuessy.

[16] See CRS Infographic IG10019, *The Freedom of Information Act (FOIA)*, by Daniel J. Sheffner.

[17] 5 U.S.C. §552(a)(1).

[18] 5 U.S.C. §552(a)(2).

[19] See also CRS Report R46238, *The Freedom of Information Act (FOIA): A Legal Overview*, by Daniel J. Sheffner. Depending on the type of information requested and purpose of the requester, fees may be assessed by agencies to help cover the costs of providing information. See CRS In Focus IF11272, *Freedom of Information Act Fees for Government Information*, by Meghan M. Stuessy for more information.

[20] Currently, Executive Order 13526 establishes this criterion. Executive Order 13526, "Classified National Security Information," 75 *Federal Register* 1013, December 29, 2009.

7. Certain records compiled for law enforcement purposes—for example, information whose release could reasonably be expected to interfere with law enforcement proceedings or would deprive a person of a right to a fair trial;
8. Information contained in or related to certain agency financial institution reports; and
9. Geological and geophysical information and data concerning wells.[21]

FOIA provides requesters with the right to file an appeal of the agency's denial of a request.[22] Disputes over the accessibility of requested records may also be resolved by consulting NARA's Office of Government Information Services through mediation.[23] A requester dissatisfied with the agency's ultimate decision may be able to seek review of the decision in federal court.[24]

Use of Exemptions

Agencies invoke certain exemptions to withhold requested information more than others.[25] The five most commonly invoked exemptions in FY2022, in order, are Exemption 6, Exemption 7(C), Exemption 7(E), Exemption 3, and Exemption 5.[26] **Table 1** provides totals for each exemption in FY2022. Some Members of Congress have recently noted the rise in the use of exemptions to withhold information, supported by findings from a 2021 Government Accountability Office (GAO) report[27] that found that "[w]hile the number of FOIA requests processed increased by 32 percent from approximately 666,000 in 2012 to 878,000 in 2019, the use of [Exemption 3] more than doubled during this time period from approximately 31,000 uses in 2012 to 72,000 in 2019 (a 135 percent increase)."[28]

Table 1. FOIA Request Exemptions by Number of Times Invoked

FY2022

Request Exemption	Number of Times Invoked
Exemption 1	2,740

[21] For more information, see CRS Report R46238, *The Freedom of Information Act (FOIA): A Legal Overview*, by Daniel J. Sheffner.

[22] 5 U.S.C. §552(a)(6)(A)(i).

[23] NARA, Office of Government Information Services, *Mediation Program*, https://www.archives.gov/ogis/mediation-program.

[24] 5 U.S.C. §552(a)(4)(B). For information on requester's ability to seek judicial review of agency withholding decisions and related issues, see CRS Report R46238, *The Freedom of Information Act (FOIA): A Legal Overview*, by Daniel J. Sheffner.

[25] CRS analysis of FOIA data located at https://www.foia.gov/data.html.

[26] Exemption 7 covers records or information compiled for law enforcement purposes. Exemption 7(C) covers information that "could reasonably be expected to constitute an unwarranted invasion of personal privacy," and 7(E) covers information that "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law."

[27] House Committee on Oversight and Reform, "GAO Reports Find Agencies Withheld More Information from the Public in Recent Years," press release, March 16, 2021, at https://oversight.house.gov/news/press-releases/gao-reports-find-agencies-withheld-more-information-from-the-public-in-recent.

[28] U.S. Government Accountability Office (GAO), *Freedom of Information Act: Update on Federal Agencies' Use of Exemption Statutes*, GAO-21-148, January 2021, p. 12, https://www.gao.gov/assets/gao-21-148.pdf. FOIA exemptions are often referred to by their *U.S. Code* subsection number, as in the cited GAO report where Exemption 3 is referred to as the "(b)(3) exemption."

Request Exemption	Number of Times Invoked
Exemption 2	1,250
Exemption 3	79,768
Exemption 4	11,276
Exemption 5	65,807
Exemption 6	287,501
Exemption 7(A)	8,041
Exemption 7(B)	311
Exemption 7(C)	256,159
Exemption 7(D)	6,154
Exemption 7(E)	242,546
Exemption 7(F)	2,143
Exemption 8	208
Exemption 9	54

Source: CRS analysis of Freedom of Information Act data, located at https://www.foia.gov/data.html.

Notes: Multiple exemptions may be invoked on a single request. The numbers provided are not equivalent to the total number of requests received in a given fiscal year.

Request Backlog

DOJ provides information through FOIA.gov and annual reports on whether requests for information are fully granted or partly granted due to the applicability of one of FOIA's exemptions as well as information on the ability of agencies to process requests in a timely way. In FY2022, 878,420 requests were processed, and in FY2021, 838,668 were processed. Comparing across years, fewer requests were fully granted in FY2022 than in FY2021 (17.4% versus 19.8%), and fewer requests received partial grants of information in FY2022 (39.1% versus 40.1%).[29]

The backlog of requests not completed by agencies continues to persist, indicating that agencies are not keeping pace with the number of requests received. **Table 2** presents the number of backlogged requests, FY2018-FY2022.

[29] DOJ, Office of Information Policy, *Summary of Annual FOIA Reports for Fiscal Year 2019*, p. 6, https://www.justice.gov/oip/page/file/1282001/download; and DOJ, Office of Information Policy, *Summary of Annual FOIA Reports for Fiscal Year 2020*, p. 7, https://www.justice.gov/oip/page/file/1436261/download. See also GAO, *Freedom of Information Act: Federal Agencies' Recent Implementation Efforts*, GAO-20-406R, March 11, 2020, p. 2, https://www.gao.gov/assets/gao-20-406r.pdf.

Table 2. Number of Backlogged FOIA Requests

Fiscal Year	Number of Requests
FY2018	130,718
FY2019	120,436
FY2020	141,762
FY2021	153,227
FY2022	206,720

Source: CRS analysis of Freedom of Information Act data, located at https://www.foia.gov/data.html.

In 2014, NARA established a FOIA Advisory Committee to develop consensus recommendations for improving the administration of FOIA.[30] The FOIA Advisory Committee has made a number of proposals to address backlog issues, such as including FOIA performance standards in employee appraisals, centralizing FOIA request processing, and adding support staff to assist with request surges.[31] In light of these recommendations, assessing the adequacy of agency resources may prove challenging, because many staff and agency components can be involved in the processing of a request, making it difficult to pinpoint where agency resources should be leveraged.

Agency FOIA Office Structures and Leadership

FOIA request backlogs may be related to the positioning of FOIA offices within agencies and the ability of chief FOIA officers to devote adequate attention to their duties. By statute, an agency's chief FOIA officer is responsible for ensuring efficient and appropriate agency-wide compliance.[32] The statute specifies that the chief FOIA officer shall be an assistant secretary or equivalent within an agency, but it is common for the person serving in the role to split his or her duties with another assistant secretary role.[33] For example, the chief FOIA officer may also serve as the agency's chief privacy or management officer, assistant secretary for public affairs, or general counsel.

Issues for Congress

Congress has amended and revised FOIA, most recently through the FOIA Improvement Act of 2016 (P.L. 114-185), and may contemplate further evaluations of the design and implementation of the law. Congress might consider options for improving the administration of FOIA in light of the use of FOIA's exemptions, reducing a persistent backlog of requests from previous years, and decreasing the number and variety of offices managing FOIA requests. Some Members of Congress have called attention to a backlog in processing FOIA requests across the government and a "continued culture of reflexive secrecy" in agencies resulting in the withholding of

[30] NARA, "Freedom of Information Act Federal Advisory Committee," https://www.archives.gov/ogis/foia-advisory-committee.

[31] NARA, Freedom of Information Act Federal Advisory Committee, *Report to the Archivist of the United States: Final Report and Recommendations,* April 17, 2018, https://www.archives.gov/files/final-report-and-recommendations-of-2016-2018-foia-advisory-committee.pdf.

[32] 5 U.S.C. §552(j). See also NARA, *Chief Freedom of Information Act (FOIA) Officers Council*, https://www.archives.gov/ogis/about-ogis/chief-foia-officers-council.

[33] 5 U.S.C. §552(f)(1).

responsive information.[34] Congress may wish to conduct oversight of the proper application of all exemptions, including content-specific exemptions written into statute under Exemption 3. Regarding the FOIA backlog, Congress may consider policies that would target FOIA backlogs at particular agencies or take a broader multiagency approach.

Lastly, the variety of duties and organizational placements of agency chief FOIA officers may pose obstacles to centralizing FOIA request processing. In some agencies, the chief FOIA officer might report directly to the agency head, while in others, the officer might be several steps removed from the agency head. Congress may wish to investigate whether these varying leadership structures are contributing to the size of FOIA request backlogs.

The Privacy Act

The Privacy Act of 1974 concerns the use and disclosure of government information collected on individuals.[35] While the other three statutes discussed in this report focus on the broad release of government information to the public, the Privacy Act instead balances the government's need to maintain and share information on individuals with the rights of individuals to be protected against invasion of their privacy.[36]

Generally, the Privacy Act prescribes how records with individually identifying information are to be stored, who may access such information, and when the government may use or share an individual's information.[37] The statute provides for 12 exceptions when information may be shared without the prior written consent of an individual.[38]

The Privacy Act allows citizens of the United States or aliens lawfully admitted for permanent residence to access and correct information collected on them and, in addition, restricts how and when these records may be shared.[39] Under the act, *record* means "any item, collection, or grouping of information about an individual that is maintained by an agency" that includes the person's name or another identifier.[40] The Privacy Act also implemented what are known as the

[34] Letter from Sens. Charles Grassley et al. to Melanie Pustay, Director, Office of Information Policy, DOJ, March 14, 2019, https://www.feinstein.senate.gov/public/_cache/files/5/f/5fdc0259-a56c-4b44-b4c5-964cd0a0cf4c/07273BBD4FF7BB01289B5E1BD329E9E2.2019-03-14-ceg-leahy-cornyn-feinstein-to-doj—foia-compliance.pdf.

[35] For more information on the Privacy Act, see CRS Report R47863, *The Privacy Act of 1974: Overview and Issues for Congress*, by Meghan M. Stuessy.

[36] For an elaboration of Congress's findings and purposes, see the Privacy Act of 1974, §2 (P.L. 93-579, December 31, 1974; 88 Stat. 1896).

[37] The Privacy Act at 5 U.S.C. §552a(4) defines *record* as "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." DOJ in its *Overview of the Privacy Act of 1974*, 2020 edition, refers to this as individually identifiable information. The Privacy Act notably does not use the term *personally identifiable information* (PII). OMB, however, has specifically defined PII as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." OMB, *M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007, https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2007/m07-16.pdf.

[38] DOJ, *Overview of the Privacy Act of 1974*, 2020, p. 80, https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition. In addition to the 12 *exceptions*, the act also stipulates 10 categories of information that are *exempted* from its purview (see page 338). However, these are omitted from discussion in this overview report.

[39] DOJ, *Overview of the Privacy Act of 1974*, pp. 421-422.

[40] 5 U.S.C. §552a(4). Other statutory definitions of *record* exist outside of the Privacy Act, such as the Federal Records Act definition, located at Title 44, Section 3301, of the *U.S. Code*.

Fair Information Practice Principles (FIPPs) in order for individuals to understand the information agencies may share pertaining to them.[41] DOJ explains that these principles

> allow individuals to determine what records pertaining to them are collected, maintained, used, or disseminated by an agency; require agencies to procure consent before records pertaining to an individual collected for one purpose could be used for other incompatible purposes; afford individuals a right of access to records pertaining to them and to have them corrected if inaccurate; and require agencies to collect such records only for lawful and authorized purposes and safeguard them appropriately. Exceptions from some of these principles are permitted only for important reasons of public policy.

In processing requests for information under the Privacy Act, agencies are also to consider the applicability of FOIA to the request. As DOJ describes, "The Privacy Act and the FOIA are often read in tandem," although the scope of each differs.[42] While FOIA allows any person to access government information, the Privacy Act allows individuals to access records about themselves. In practice, agencies treat Privacy Act requests the same as FOIA requests when preparing responses. DOJ recommends that agencies process individuals' access requests for their own records "under both the Privacy Act and the FOIA, regardless of the statute(s) cited."[43]

"System of Records"

For purposes of the Privacy Act, an agency may control a group of records where information is retrievable by an individual's name or other unique identifier. This group of records is referred to as a "*system of records*."[44] The act requires an agency to submit a proposal to OMB and Congress for review on the establishment of or significant changes to a system of records.[45] After review and potential comments from OMB, the agency publishes a system of records notice (SORN) in the *Federal Register* and provides 30 days for the public to submit written views on the proposed use of the system.[46] A typical SORN must include information such as

- the name and location of the system;
- the categories of records and individuals on whom records are maintained;
- each routine use of the records contained in the system, including the categories of users and the purpose of such use; and
- the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records.[47]

[41] DOJ elaborates, "Judicial redress is afforded to individuals when an agency fails to comply with access and amendment rights, but only after an internal appeals process fails to correct the problem. Otherwise, liability for damages is afforded in the event of a willful or intentional violation of these rights." DOJ, *Overview of the Privacy Act of 1974*, p. 1.

[42] DOJ, *Overview of the Privacy Act of 1974*, p. 138. For an example of this process, see pages 141-147 of the cited document.

[43] DOJ, *Overview of the Privacy Act of 1974*, p. 139.

[44] 5 U.S.C. §552a(a)(5).

[45] OMB, *Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, December 23, 2016, p. 14, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A108/omb_circular_a-108.pdf.

[46] 5 U.S.C. §552a(e)(11). OMB guidance indicates that this requirement refers to "any new or significantly modified routine use." OMB, *Circular No. A-108*, p. 7.

[47] 5 U.S.C. §552a(e)(4).

Certain systems of records may be exempted from selected Privacy Act requirements by an agency head based on the system's contents and subject to notice in the *Federal Register*.[48] For example, systems containing national security information, investigatory material compiled for law enforcement purposes, or information required by statute to be maintained and used solely as statistical records may be exempted in certain circumstances.[49]

Access to Information on Individuals

U.S. citizens and permanent residents may request to gain access to their information from agencies under the same guidelines as requests under FOIA.[50] An individual may request an agency to perform a search for information in a system of records based on identifiers such as a name or Social Security number. An individual might do this, for example, to ensure records pertaining to the individual are accurate and to request corrections.

The Privacy Act generally prohibits disclosure of individually identified information to third parties without written consent. Specifically, an agency may not disclose a record to a third party without the individual's prior written consent unless a disclosure meets an exception under Title 5, Section 552a(b), of the *U.S. Code*.[51] Congress has enacted legislation to digitize the collection of written consent under the Privacy Act, but the verification of an individual's identity may vary based on whether the consent is granted via digital or paper means.[52] For example, while implementation of digital consent collection is ongoing and subject to OMB guidance, paper consent may involve document notarization or a signature offered under penalty of perjury.[53]

Two of the exceptions allowed by the statute have raised congressional concern. An agency may share information if the purpose of the sharing is a "routine use" of the information. A routine use, under the Privacy Act, is "use of such record for a purpose which is compatible with the purpose for which it was collected" and may include the sharing of information across agencies.[54] Determining a qualifying routine use is often left to the discretion of agencies and OMB, although routine uses must be noted and defined in publicly available SORNs.[55]

The "routine use" disclosure exception was designed to allow disclosures other than intra-agency disclosures.[56] As described by DOJ, "The routine use exception, because of its potential breadth, is one of the most controversial provisions in the Act."[57] This exception allows for agencies to

[48] 5 U.S.C. §§552a(j) and 552a(k). For discussion of statutory provisions that explicitly exempt or allow agencies to exempt certain categories of records (or information within a record) from certain Privacy Act provisions, see DOJ, *Overview of the Privacy Act of 1974*, "Ten Exemptions," https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/exemptions; and OMB, *Circular No. A-108*, p. 25.

[49] 5 U.S.C. §552a(k).

[50] 5 U.S.C. §552a(d).

[51] 5 U.S.C. §552a(b). For discussion of these exceptions, see DOJ, *Overview of the Privacy Act of 1974*, "Conditions of Disclosure to Third Parties," https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/disclosures-third-parties.

[52] P.L. 116-50.

[53] OMB, *M-21-04: Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act*, November 12, 2020, https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-04.pdf; and NARA, "Guide to Making a Privacy Act Request: What Is a Privacy Act Certification of Identity?," https://www.archives.gov/privacy/guide.html.

[54] 5 U.S.C. §552a(a)(7).

[55] OMB, *Circular No. A-108*, p. 11.

[56] DOJ, *Overview of the Privacy Act of 1974*, p. 95.

[57] DOJ, *Overview of the Privacy Act of 1974*, p. 95.

make certain disclosures of information under its provisions that may not otherwise be captured through the Privacy Act's other exceptions.[58]

An agency may also disclose information for use in statistical research. The Privacy Act states that the recipient of this information must provide the agency with "advance adequate written assurance that the record will be used solely as a statistical research or reporting record" and that the information is to be "transferred in a form that is not individually identifiable."[59] The OMB stated in its initial 1975 guidelines on the Privacy Act's implementation:

> One may infer from the legislative history and other portions of the Act that an objective of this provision is to reduce the possibility of matching and analysis of statistical records with other records to reconstruct individually identifiable records. An accounting of disclosures is not required when agencies publish aggregate data so long as no individual member of the population can be identified.[60]

Issues for Congress

In the Privacy Act's 1974 enumeration of findings and purposes, Congress found that "the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information."[61]

As technology advances, opportunities for use and misuse of systems of records may be present in ways not considered during the original design and implementation of the Privacy Act. Congress has passed legislation providing further direction on the sharing and storage of information maintained on individuals. Examples of legislation that interact with the Privacy Act include provisions associated with the Computer Matching and Privacy Protection Act of 1988 and subsequent amendments[62] and the Confidential Information Protection and Statistical Efficiency Act of 2018 (CIPSEA 2018), which was included in Title III of the Foundations for Evidence-Based Policymaking Act of 2018 (FEBPA).[63]

Privacy Act and the Mosaic Effect

Given existing and emerging computer technologies at the time of its consideration, the Privacy Act included numerous safeguards to avoid privacy-related harms to the public. Data access and sharing may still involve significant risks even with seemingly de-identified data. OMB has warned of the *mosaic effect*, a problem that could occur as multiple versions of public and private

[58] For example, the National Endowment for the Arts announced eight routine uses for a new system of records regarding medical and/or religious accommodations of its employees. The routine uses include disclosures to courts, contractors, and designated officers of other agencies for certain purposes, among other uses. National Endowment for the Arts, "Privacy Act of 1974; System of Records," 87 *Federal Register* 14298, March 14, 2022. See also DOJ, *Overview of the Privacy Act of 1974*, pp. 105-107.

[59] 5 U.S.C. §552a(b)(5).

[60] OMB, "Privacy Act Implementation: Guidelines and Responsibilities," 40 *Federal Register* 28954, July 9, 1975, https://www.justice.gov/archives/paoverview_omb-75/download. Modern privacy guidance from OMB can be located at Office of Information and Regulatory Affairs, "Privacy," https://www.whitehouse.gov/omb/information-regulatory-affairs/privacy/.

[61] Privacy Act of 1974, §2 (P.L. 93-579, December 31, 1974; 88 Stat. 1896).

[62] P.L. 100-503 (1988) and subsequent amendments to its provisions. This law inserted many new requirements in provisions associated with the Privacy Act (5 U.S.C. §522a). See also CRS In Focus IF12053, *Federal Data Integration and Individual Rights: The Computer Matching and Privacy Protection Act*, by Natalie R. Ortiz.

[63] P.L. 115-435 (2019). FEBPA's Title III codified CIPSEA 2018 at Title 44, Chapter 35, of the *U.S. Code* and replaced an earlier, 2002 version of CIPSEA.

information on individuals become accessible on the internet or through other channels. In a 2013 memorandum to agencies, OMB explained:

> The mosaic effect occurs when the information in an individual dataset, in isolation, may not pose a risk of identifying an individual (or threatening some other important interest such as security), but when combined with other available information, could pose such risk. Before disclosing potential [personally identifiable information] or other potentially sensitive information, agencies must consider other publicly available data—in any medium and from any source—to determine whether some combination of existing data and the data intended to be publicly released could allow for the identification of an individual or pose another security concern.[64]

The ubiquity of digital information has created increased privacy risks, and there is no consensus whether the shared or combined information can be destroyed in the same manner as paper records. In considering the role of the Privacy Act, Congress may wish to consider whether the current SORN process sufficiently identifies and communicates privacy risks associated with the linking and dissemination of de-identified information inside and outside the federal government.

Oversight of Information Access and Sharing Under the Privacy Act's Exceptions[65]

The Privacy Act's process for SORNs is intended to establish a baseline for transparency and accountability for agencies. Nevertheless, changes in OMB's implementation guidance could affect whether and how agencies notify Congress and the public of certain uses and changes.[66] Congress might consider oversight or legislation to assess whether or not agencies accurately characterize information uses and consistently implement the SORN process government-wide or across programmatic areas.

In response to the Privacy Act, OMB guidance to agencies provides for a largely decentralized approach for making SORNs available to Congress and the public. Agencies are directed to post SORNs and other information on their websites.[67] In addition, agencies are directed to give notice to certain congressional committees about some actions.[68] Given the potential range and volume of information use, access, and sharing under the Privacy Act's exceptions, Congress might evaluate the effectiveness of available options for oversight. Revised approaches may be more

---

[64] OMB, *Open Data Policy-Managing Information as an Asset*, M-13-13, May 9, 2013, pp. 4-5, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2013/m-13-13.pdf. OMB defines personally identifiable information, or PII, as

> information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available (in any medium and from any source) that, when combined with other available information, could be used to identify an individual.

OMB, *Guidance for Agency Use of Third-Party Websites and Applications*, M-10-23, June 25, 2010, p. 8, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2010/m10-23.pdf.

[65] Clint Brass, Specialist in Government Organization and Management, contributed to this section of the report.

[66] OMB, *Circular No. A-108*, pp. 5-13, referring to a requirement for a SORN when "making *significant* changes to an existing system of records" (p. 5) or proposing "*significantly* modified routine uses" (p. 7).

[67] OMB, *Circular No. A-108*, p. 25.

[68] OMB, *Circular No. A-108*, p. 13.

informative or less labor intensive (e.g., mandating a database to track agency ownership, flows, and uses of systems of records) to assist Congress in its oversight responsibilities.

Some have expressed concern that Title III of FEBPA effectively created a new exception to the Privacy Act without amending the Privacy Act. Specifically, Title III requires agencies to make data identifying individuals available upon request to any designated statistical agency or unit, and it allows OMB to designate statistical agencies or units at any executive agency.[69] While Title III contemplates the sharing and use of identified data "for purposes of developing evidence" to support policymaking, the law does not specify how long the shared data may exist. Congress has historically raised concerns about aggregating information into "data warehouses," which may raise issues about the design and implementation of Title III.[70]

The Government in the Sunshine Act

The Government in the Sunshine Act opens the policymaking deliberations of "collegially headed" federal agencies, boards, commissions, and councils to public scrutiny unless those deliberations are closed in accordance with any of the act's 10 exemptions. The Sunshine Act does not directly define what entities are considered collegially headed, but it does define *agency* and *meeting* for the purposes of its disclosure requirements.

- *Agency* is defined as any agency, as defined by FOIA, "headed by a collegial body composed of two or more individual members, a majority of whom are appointed by the President with the advice and consent of the Senate, and any subdivision thereof."[71]
- *Meeting* is defined as "the deliberations of at least the number of individual agency members required to take action on behalf of the agency where such deliberations determine or result in the joint conduct or disposition of official agency business."[72]

The Sunshine Act includes 10 exemptions that allow deliberations to be closed to the public. The exemptions bear many similarities to the nine exemptions of FOIA.[73] Under the Sunshine Act, agencies are required to publicly announce meetings, typically in the *Federal Register*, at least one week beforehand and include information on the meeting's time, place, and subject matter; whether it is open or closed to the public; and the name and phone number of the agency official to respond to additional requests for information.[74] Disputes over proper public notice of such meetings or the propriety of closing a deliberation may be pursued in federal court.[75]

Issues for Congress

Agencies subject to the Sunshine Act may make use of what are known as "safe harbor" options, which are not specifically authorized in statute, to circumvent the act's requirements by holding activities that do not fall within the statute's "meeting" definition. An Administrative Conference

[69] 44 U.S.C. Chapter 35, Subchapter III, Part D, including 44 U.S.C. §3581.

[70] For additional discussion, see CRS Insight IN11717, *Proposals for a National Secure Data Service, in Context*, by Meghan M. Stuessy and Clinton T. Brass.

[71] 5 U.S.C §552b(a)(1).

[72] 5 U.S.C §552b(a)(2).

[73] 5 U.S.C §552b(c).

[74] 5 U.S.C §552b(h).

[75] 5 U.S.C §552b(h).

of the United States report noted, "As a general matter, these 'safe harbors' take advantage of the quorum requirement under the Act: so long as any given interaction involves less than a quorum of members engaging in group consideration of a substantive issue, the Sunshine Act is not triggered."[76] The "safe harbors" utilized by these agencies include

- *Notational voting*, where members receive written materials, review the same independently, and then provide their votes in writing;
- *Staff meetings*, where matters are discussed at the staff or representative level and reported back to agency decisionmakers; and
- *Seriatim meetings*, a series of meetings between small groups of commissioners or board members, none of which involves a sufficiently large number of participants to comprise a quorum.[77]

Although these safe harbors may allow for more candid and free-flowing discussion, overuse or misuse of these options could inhibit the original transparency motivations behind the implementation of the Sunshine Act. While open and closed meetings are subject to *Federal Register* requirements, there are no mechanisms to reveal the use of safe harbors that do not meet the statutory criteria of a meeting. Accordingly, Congress might examine the frequency of use of these safe harbors and what bodies or contexts make the most use of them. Congress may wish to conduct oversight to determine if these safe harbors undermine the transparency called for in the Sunshine Act and consider further legislation to limit them.

The Federal Advisory Committee Act

Congress and the executive branch have created or used advisory entities within the executive branch to incorporate different perspectives in the federal policymaking process. These entities can appear as a formal federal advisory committee, an ad hoc working group, or a group of industry experts an agency must consult with. Certain characteristics of these entities or groups may trigger the requirements of the Federal Advisory Committee Act, which governs the operation and oversight of federal advisory entities.[78]

While other statutes in this report rely on request-based or proactive disclosure approaches to access to information, FACA not only allows for the opening of certain policy debates to the public; it also permits nonfederal officials to participate in the federal decisionmaking process in an advisory capacity. Generally, FACA applies to entities established to assist executive branch policymaking and grantmaking, which are typically housed within executive branch agencies and

[76] Reeve T. Bull, *The Government in the Sunshine Act in the 21st Century*, Administrative Conference of the United States, March 10, 2014, p. 9, https://www.acus.gov/sites/default/files/documents/Government%20in%20the%20Sunshine%20Act%20Draft%20Report%20REVISED%205-7-14.pdf.

[77] Bull, *The Government in the Sunshine Act in the 21st Century*, pp. 9-11.

[78] For more information on committees subject to FACA, see CRS Report R44232, *Creating a Federal Advisory Committee in the Executive Branch*, by Meghan M. Stuessy.

have a membership not wholly composed of federal officials.[79] Congress may also specifically dictate in statute whether or not FACA applies to a particular entity.[80]

Entities subject to FACA are required to meet formal reporting and oversight procedures, including

- meetings must be open and materials be available to the public;[81]
- members of the committee must be "fairly balanced" in terms of the points of view represented and the functions to be performed by the advisory committee;[82] and
- the function of advisory committees should be advisory only.[83]

The General Services Administration (GSA) maintains and administers management guidelines for federal advisory entities subject to FACA.[84] GSA's regulation for FACA, which is known as the FACA Final Rule, addresses many advisory committee meeting procedures. FACA requires an entity to file a public charter with GSA, which must include, among other information, the advisory committee's mandate and duties, frequency of meetings, and membership requirements. The entity's meetings must also be open to the public unless certain requirements are met.[85] The entity's records are also generally required to be accessible to the public.[86]

Entities that are subject to FACA are listed in GSA's online, publicly accessible FACA database. In a given fiscal year, approximately 1,000 such committees are active.[87]

Issues for Congress

Some federal advisory committees have embraced the use of virtual meetings, especially in response to coronavirus exposure concerns.[88] GSA's regulation for FACA clarifies that any advisory committee that plans a meeting "conducted in whole or in part by a teleconference, videoconference, the Internet, or other electronic medium" must announce the meeting at least 15

[79] 5 U.S.C. §1001(2). Specifically, this section reads, "The term 'advisory committee' means a committee, board, commission, council, conference, panel, task force, or other similar group, or any subcommittee or other subgroup thereof (hereafter in this paragraph referred to as 'committee') that is established or utilized to obtain advice or recommendations for the President or one or more agencies or officers of the Federal Government and that is—(i) established by statute or reorganization plan; (ii) established or utilized by the President; or (iii) established or utilized by one or more agencies.

(B) Exclusions.—The term 'advisory committee' excludes—(i) a committee that is composed wholly of full-time, or permanent part-time, officers or employees of the Federal Government; and (ii) a committee that is created by the National Academy of Sciences or the National Academy of Public Administration."

[80] For example, Section 60602 of P.L. 117-58, the Infrastructure Investment and Jobs Act, states, "The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the telecommunications interagency working group."

[81] 5 U.S.C. §1009(a)(1). Meetings may be closed under the provisions of the Sunshine Act (5 U.S.C. §552b).

[82] 5 U.S.C. §1004(b)(2).

[83] 5 U.S.C. §1002(b)(6).

[84] GSA, "Federal Advisory Committee Management," 66 *Federal Register* 139, July 19, 2001, https://www.gsa.gov/cdnstatic/FACAFinalRule_R2E-cNZ_0Z5RDZ-i34K-pR.pdf.

[85] 5 U.S.C. §1009.

[86] 5 U.S.C. §1010.

[87] CRS search of the GSA FACA Database, located at http://www.facadatabase.gov.

[88] For example, see Environmental Protection Agency, "Great Lakes Advisory Board Notice for Virtual Meeting," 86 *Federal Register* 68251-68252, December 1, 2021.

calendar days in advance in the *Federal Register*, provide an agenda of the meeting, and comply with the requirements of the Sunshine Act.[89]

Questions may remain, however, about what virtual access to meetings could mean. For example, must meetings be conducted with a particularly accessible or free software application? In addition, must the software allow for written or verbal public comment? At present, the FACA Final Rule directs agencies to plan for a designated public call-in line for a teleconference but is otherwise silent on videoconference capacities to be considered.[90] Congress might consider options to clarify or expand the requirements for digital meetings in keeping with the statute's goal of providing for public policy debate within committees.

Policy Considerations and Balancing Values

Access over Time

As methods of information storage and technologies continuously evolve, the span of time from information creation to retrieval can impact the ways in which information is accessed. Government information may also have a fuller or different meaning if the information is disclosed during contemporaneous events rather than as a historical matter later on. In some instances, relevant statutes prohibit disclosure of particular categories of information for specified periods of time. One example is the Presidential Records Act (44 U.S.C. §§2201-2207), which embargoes certain presidential records from access by the public for specific periods of time after the conclusion of a presidency.[91] Additional questions considering the impact of time on information access could be categorized as follows:

- **Effects on agency decisionmaking.** For example, might the timing of information release bring additional urgency to the matters being decided by an agency? Conversely, might a delay in the release skew the context in which the information was created?
- **Effects on individual privacy or confidentiality.** How does the passage of time alter the impact of information released about individuals, and how might it affect individual privacy? Are privacy concerns, for example, the same for those seeking federal benefits or judicial relief as they are for the deceased?
- **Effects on information stewardship.** Depending on the length of the delay, the information and the media on which it was recorded—analog or digital—may be degraded and no longer readable.

Scholar Jean-François Blanchette notes that digital information is often considered by the public to be devoid of the physical limitations and degradation considerations that typify traditional media:

> In this characterization, the digital derives its power from its nature as a mere collection of 0s and 1s wholly independent from the particular media on which it is stored—hard drive, network wires, optical disk, etc.—and the particular signal carrier which encodes bits—variations of magnetic field, voltages, or pulses of light. This purported immateriality endows bits with considerable advantages: they are immune from the economics and

[89] GSA, "Federal Advisory Committee Management," 66 *Federal Register* 37745.

[90] GSA, "Federal Advisory Committee Management," 66 *Federal Register* 37731.

[91] For more discussion of this process, see CRS Report R46129, *The Presidential Records Act: An Overview*, by Meghan M. Stuessy.

> logistics of analog media, and from the corruption, degradation, and decay that necessarily result from the handling of material carriers of information, resulting in a worldwide shift "from atom to bits" as captured by Negroponte. This is problematic: however immaterial it might appear, information cannot exist outside of given instantiations in material forms.[92]

Congress may consider strategies and methods for managing digital media in similar ways to the management of analog media. The timing of when information is released, therefore, may often matter as much as what information is released.

Mitigating Factors of Transparency

Government agencies contend that expecting perfect transparency is unrealistic and may hinder agencies' ability to work efficiently or speak candidly internally about policy matters.[93] Studies have identified other consequences of scrutiny, including delays in the completion of tasks, increases in time that personnel spend responding to scrutiny rather than performing regular duties, and reduced creativity in addressing challenges. These may be balanced to some extent by a greater diligence to completing announced activities.[94]

Congress has asserted the need to balance these concerns with the public's right to know through consideration of exceptions to transparency requirements and the ability to close meetings in limited instances. The Senate Committee on Governmental Affairs in 1989 reported:

> Congress concluded that for the most part the fears advanced by the agencies were unfounded…. Second, Congress determined that the values inherent in open government vastly outweighed any concerns, whatever their validity, about "chilling" agency deliberations.[95]

Policymakers may wish to continue to evaluate whether these exceptions strike the correct mix to provide transparency and allow for unfiltered discussion.[96]

For Additional Reading

Reeve T. Bull, *The Government in the Sunshine Act in the 21st Century*, Administrative Conference of the United States, March 10, 2014, https://www.acus.gov/sites/default/files/documents/Government%20in%20the%20Sunshine%20Act%20Draft%20Report%20REVISED%205-7-14.pdf.

---

[92] For further discussion, see Jean-François Blanchette, "A Material History of Bits," *Journal of the Association for Information Science and Technology*, vol. 62, no. 6 (April 19, 2011), pp. 1042-1057.

[93] Bull, *The Government in the Sunshine Act in the 21st Century*, p. 3.

[94] For discussion, see Robert I. Sutton and D. Charles Galunic, "Consequences of Public Scrutiny for Leaders and Their Organizations," in Barry M. Staw and Larry L. Cummings, eds., *Research in Organizational Behavior*, vol. 18 (Greenwich, CT: JAI Press, 1996), pp. 201-250.

[95] U.S. Congress, Senate Committee on Governmental Affairs, *Government in the Sunshine Act: History and Recent Issues*, committee print, 101st Cong., 1st sess., November 1, 1989, S.Prt. 101-54 (Washington: GPO, 1989), p. 33.

[96] In regard to the Sunshine Act, discussed earlier in this report, Senator Lowell Weicker explained, "We have heard all the arguments against the bill from the commissions and agencies whose operations this bill would bring to light. The points they raise run the gamut from: the bill would unnecessarily inhibit the efficient conduct of an agency business to beliefs that this bill would not allow a free and open exchange of ideas and candid opinions. What they seem to forget is the overriding responsibility to allow the public, in order for them to participate in the decision-making process, to have an unfettered access to information on how their government operates." U.S. Congress, Senate Committee on Governmental Affairs, *Government in the Sunshine Act: History and Recent Issues*, committee print, 101st Cong., 1st sess., November 1, 1989, S.Prt. 101-54 (Washington: GPO, 1989), p. 33.

U.S. Congress, House Committee on Oversight and Government Reform, *A Citizen's Guide to Using the Freedom of Information Act and the Privacy Act to Request Government Records*, committee print, 112th Cong., 2nd sess., September 21, 2012, H.Rept. 112-689, https://www.congress.gov/112/crpt/hrpt689/CRPT-112hrpt689.pdf.

DOJ, *FOIA.gov*, http://www.foia.gov/about.html.

DOJ, Office of Privacy and Civil Liberties, *Overview of The Privacy Act of 1974*, 2020, https://www.justice.gov/Overview_2020/download.

DOJ, *United States Department of Justice Guide to the Freedom of Information Act*, https://www.justice.gov/oip/doj-guide-freedom-information-act-0.

GSA, "Federal Advisory Committee Management," 66 *Federal Register* 139, July 19, 2001, https://www.gsa.gov/cdnstatic/FACAFinalRule_R2E-cNZ_0Z5RDZ-i34K-pR.pdf.

GSA, *Federal Advisory Committee Act (FACA) Management Overview*, https://www.gsa.gov/policy-regulations/policy/federal-advisory-committee-act-faca-management-overview.

GSA, *GSA Federal Advisory Committee Act (FACA) Database*, https://www.facadatabase.gov/FACA/FACAPublicPage.

OMB, *Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, December 23, 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A108/omb_circular_a-108.pdf.

Author Information

Meghan M. Stuessy
Analyst in Government Organization and Management

Disclaimer